企业网络安全防范系统的研究设计与实现

摘　要

近年来，计算机网络信息技术更新迭代飞速发展，现已覆盖到了生活中的各个方面，给这个时代带来了极大的便利。但同时，网络当中的安全隐患也是普遍存在的。由于 PC 系统存在一定的漏洞，使得计算机会遭受到外部的恶意攻击，因此网络安全逐渐成为我们使用计算机时重点关注的一个问题。防火墙作为保护日常生活中网络安全的一种重要技术手段，它能够防御我们平时遇到的很多网络安全问题，在企业网络安全中被广泛使用。

本文主要分析了国内企业网络的安全现状。通过结合公司网络当前的状况，公司网络安全保护系统的当前问题和隐患从公司本身开始针对安全技术，网络保护和公司安全管理。介绍了云平台的开发及其他方面的深入研究和分析，以及针对性的特定解决方案，最后建立了一个全面的网络安全保护系统，用于物理保护和云平台保护的集成。应用的网络安全技术有访问控制技术，身份认证技术，防火墙，防病毒软件，加密技术等。对安全系统进行部署和升级后，对运行结果的分析表明，该安全系统可以满足“保护信息安全级别的基本要求”，可以有效地防范来自各个方面的攻击和威胁，使其更加健壮。

关键词：运行安全；数据采集；实时监控；网络安全

ABSTRACT

In recent years, the rapid development of computer network information technology has iterated and it has covered all aspects of life, which has brought great convenience to this era. But at the same time, hidden security risks in the network are also widespread. Due to certain loopholes in the PC system, the computer will be subject to external malicious attacks, so network security has gradually become an issue that we focus on when using computers. As an important technical means to protect the network security in daily life, the firewall can prevent many network security problems that we usually encounter, and is widely used in corporate network security.

This article mainly analyzes the security status of domestic corporate networks. By combining the current situation of the company's network, the current problems and hidden dangers of the company's network security protection system start from the company itself for security technology, network protection and company security management. Introduced the in-depth research and analysis of cloud platform development and other aspects, as well as targeted specific solutions, and finally established a comprehensive network security protection system for the integration of physical protection and cloud platform protection. The applied network security technologies include access control technology, identity authentication technology, firewall, antivirus software, and encryption technology. After the deployment and upgrade of the security system, the analysis of the operating results shows that the security system can meet the "basic requirements for protecting the level of information security" and can effectively prevent attacks and threats from all aspects, making it more robust.

Key words: operational safety; data collection; real-time monitoring; network security

第 1 章 绪论

1.1 研究背景与意义

随着互联网的发展，很多企业都受益于计算机网络系统的高效的办公效率。但由于计算机网络中存在很多不安全因素，因而计算机技术，通信技术和一些高端产业的发展都需要网络安全技术的支撑。计算机网络已逐渐覆盖不同的学校，企业或个人和家庭。它丰富了学生们的教学内容和校园生活，优化完善企业商务系统，彻底改变了以往人们的生活态度和休闲方式。如今计算机网络进入了我们的日常工作和学习，并已成为不可缺少的一部分。无论系统多么完美，仍然存在问题，我们必须注意网络安全性。该公司高效，协作和完善的运营和管理受益于信息交换，实时传输和网络系统功能，这些功能消除了诸如距离之类的高质量功能。互联网时代，企业的日常管理必须依靠信息系统和网络才能够更好的发展。但，凡事总是利弊相兼的，计算机网络系统带来便利的同时也存在一部分安全问题，如病毒，木马，系统的漏洞，恶意软件还有硬件和软件的不兼容等。网络的健康发展道路之所以如此坎坷，主要原因是缺乏网络系统使用的技术手段，以及缺乏对网络安全防范措施的意识，所有这些都使人们关注公司信息的安全性。因此，我们不应该忽视计算机网络的安全性，必须认真对待它们它。为了避免网络安全遭到破坏，很多企业购买防火墙搭建防御系统的，在内网与外网之间建立一道屏障，保护公司内部网络系统免于遭遇外部攻击，从根本上保障外部信息安全流入公司，防止内部网络系统受到攻击。在防火墙的外部防御过程中，以相对较低的安全性阻止数据是最基本的链接。整个连接取决于过滤器规则，这些规则最终由防火墙的安全策略制定。随着时间的不断发展，人们对网络安全的认识逐渐提高。且已经学会了使用防火墙来保护隐私和网络安全，但是黑客的入侵并未停止。从这些各种威胁因素中不难发现，如果只是在企业网络安全系统中配置一些简单的防御技术，只能解决计算机网络中的少部分威胁。而且，随着网络技术的不断变化，各种不同的网络攻击方法也在不断发生着变化，网络病毒也在不断更新。为了找到防御这些病毒防御技术，我们还需要不断加强和更新相应的方法